BNA

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Personal Information

California Data Security

Businesses that own or license personal information about California residents must implement ''reasonable security procedures'' to protect that information under A.B. 1950, a bill recently signed into law in California. The new law builds on California's S.B. 1386, which went into effect in July 2003, and requires state agencies and firms that conduct business in California to notify California consumers of security breaches that may have compromised the integrity or confidentiality of their computerized personal information. While the scope of S.B. 1386 is limited to a notification duty, A.B. 1950 addresses the duty to maintain adequate security.

New California Information Security Law Will Have National Impact

BY REECE HIRSCH

On Sept. 29, 2004, California Gov. Arnold Schwarzenegger (R) signed a bill that will impose new information security obligations on a wide range of companies that receive personal information of California residents. As with many of the other recent California privacy and security laws, the new law, Assembly Bill 1950, will have an impact that extends far beyond California's borders.

Reece Hirsch is a partner in the San Francisco office of Sonnenschein Nath & Rosenthal LLP. He can be reached at rhirsch@sonnenschein.com or (415) 882-5040.

Just as a spate of California outsourcing-related privacy bills were triggered in large part by a single, widely reported incident involving a Pakistani medical records transcriptionist, the Assembly analysis of A.B. 1950 states that the measure was prompted by an incident in which documents containing sensitive personal information were mistakenly used as props in a Los Angeles-based television production.

Overview. A.B. 1950 requires that a business that owns or licenses personal information about a California resident implement and maintain reasonable secu-

rity procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification or disclosure. The new law amends Title 1.81 of the California Civil Code at Section 1798.81.5.

The statute also provides that a business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.

As with other recent California privacy and security laws, such as S.B. 1386, the security breach notification statute, A.B. 1950 is likely to influence organization-wide security practices for many companies with national operations. Because it may not be possible for a business to segregate the personal information of its California customers, the reasonable security practices mandated by A.B. 1950 will often be applied to all customer information maintained by a business.

Companies Exempted From Compliance. A.B. 1950 is intended to ''fill the gaps'' left by certain industry-specific privacy and security laws. The law does not apply to: (i) health care providers, health plans and contractors regulated by the Confidentiality of Medical Information Act (CMIA), California's medical privacy law; (ii) ''financial institutions'' regulated under California law; (iii) covered entities governed by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); and (iv) entities subject to the confidentiality requirements of the California Vehicle Code with respect to Department of Motor Vehicles records.

In addition, if a business is already regulated by another state or federal law that provides greater protection for personal information than A.B. 1950, then compliance with that law will be deemed compliance with A.B. 1950. For example, an insurance company licensed by a state other than California may be subject to security requirements imposed under insurance regulations promulgated under the Gramm-Leach-Bliley Act (GLBA). If these insurance regulations provide ''greater'' protection than A.B. 1950, then the insurance company will be considered compliant with A.B. 1950 with respect to personal information of California residents that it receives.

Personal Information. A.B. 1950 defines ''personal information'' as an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (i) Social Security number; (ii) driver's license number or California identification card number; (iii) account number, credit card or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account; and (iv) medical information.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records. A.B. 1950's definition of personal information is the same as the definition adopted in S.B. 1386, California's security breach notification law, except for the inclusion of ''medical information.''

A.B. 1950 applies to businesses that ''own or license'' personal information, but the statute provides no guidance regarding the meaning of those terms. Information that a business maintains regarding its customers and their transactions will almost certainly constitute ''owned or licensed information.'' It is likely that employee records maintained by the Human Resources department of a business would also qualify.

Reasonable Security Procedures and Practices. A.B. 1950 imposes on businesses a requirement to maintain ''reasonable'' security procedures and practices appropriate to the nature of the information. The law does not, however, provide any guidance as to what security procedures and practices may be deemed appropriate.

A.B. 1950 is likely to fall primarily under the jurisdiction of the California Office of Privacy Protection. The privacy protection office issued guidance regarding compliance with the California security breach notification law (S.B. 1386), but it does not currently contemplate issuing a best practices guide for A.B. 1950.

In the absence of clear guidance regarding the meaning of ''reasonable'' security measures, businesses subject to A.B. 1950 should reevaluate their security practices in light of a variety of potentially relevant legal and industry standards, including the HIPAA Security Rule, GLBA, California S.B. 1386 and guidance issued by organizations such as the National Institute of Standards and Technology (NIST).

Contracts With Third Parties. As noted above, A.B. 1950 requires that a business subject to the statute that shares personal information with a nonaffiliated third party must enter into to a contract requiring that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure. Once again, the statute does not provide specific guidance regarding the terms of such agreements.

Businesses required to enter into contracts pursuant to A.B. 1950 would be well served to consider the terms of HIPAA business associate agreements and GLBA service provider agreements as a starting point.

A.B. 1950 and HIPAA Business Associate Agreements. Some of the complexities of A.B. 1950 become apparent when applying the law to business associate relationships under HIPAA. A business associate relationship generally exists when an individual or entity, acting on behalf of a HIPAA-covered entity, assists in the performance of a function or activity involving the use or disclosure of protected health information. A.B. 1950 exempts HIPAA-covered entities from compliance, but it does not exempt business associates.

HIPAA-covered entities are required to enter into agreements requiring their business associates to ''implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability'' of electronic protected health information received from the covered entity. For those HIPAA business associates that are also subject to A.B. 1950, the California law creates a new, independent legal obligation with respect to security beyond the terms of the business associate agreement.

  PVLR ISSN 1538-3423

California medical privacy law complicates this analysis. A.B. 1950 also exempts ''contractors'' subject to the CMIA, which include medical groups and other ''medical service organizations.'' The CMIA imposes certain confidentiality requirements upon contractors with respect to medical information. Therefore, if a business is a ''contractor'' under the CMIA, it will be exempt from A.B. 1950, despite the fact that it may also be a ''business associate'' under HIPAA.

Private Right of Action. Although A.B. 1950 does not specifically address standing, a private right of action will be available for violations of the law under California's unfair competition law. California Business and Professions Code Section 17200 generally permits a private party to bring a lawsuit for any business practice that is otherwise forbidden by law or deemed to constitute an unfair business practice, even if that law does not expressly provide for a private right of action. A Section 17200 lawsuit may be brought as a class action.

It is noteworthy that any unauthorized access to, or use of, personal information may constitute a violation of A.B. 1950, even if no actual harm results. However, Committee staff have stated that A.B. 1950 should not form the basis for a cause of action if reasonable security practices and procedures have been implemented.